# Figure 1

108

104

102
Network

Client

110

Client

100

112

Client

Server

Storage

106

---

Processor
202

Processor
204

206

System Bus

208

Memory
Controller/
Cache

I/O Bridge

210

# Figure 2

200

Local Memory
209

212

PCI Bus
Bridge
214

216

PCI Bus

218

Modem

Network
Adapter

220

Graphics
Adapter
230

I/O Bus

PCI Bus
Bridge
222

PCI Bus

226

Hard Disk
232

PCI Bus
Bridge
224

228

PCI Bus

# Figure 3

Black et al.
AUS920010291US1
Method and Apparatus in a Data
Processing System for Managing
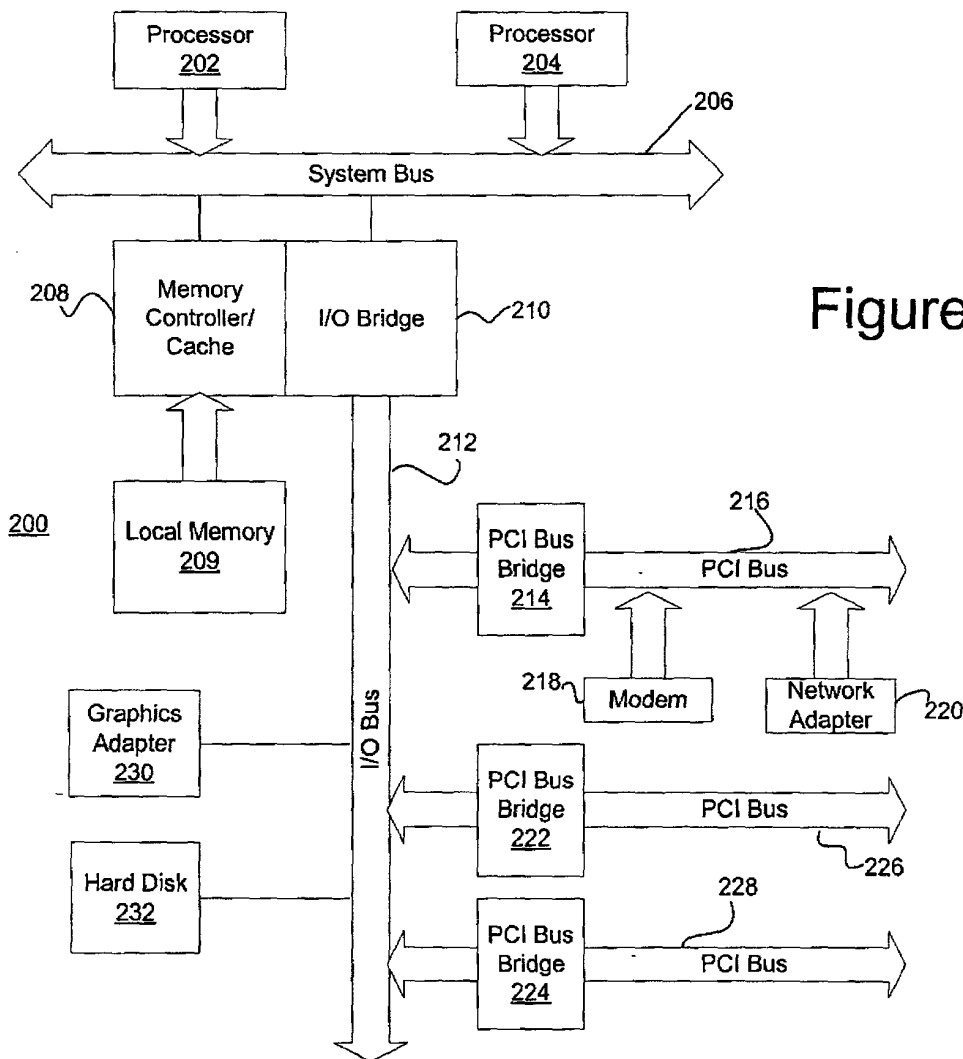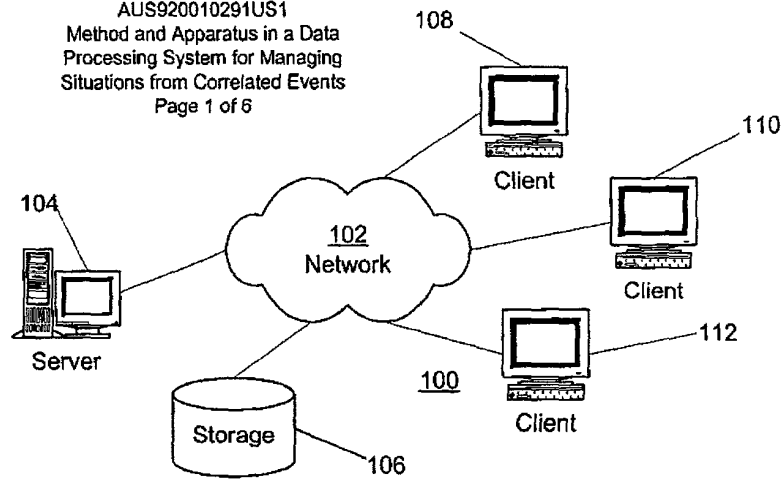Situations from Correlated Events
Page 2 of 6

Client
300

Processor
302

Host/PCI
Cache/
Bridge

308

Main Memory
304

Audio
Adapter
316

Bus    306

SCSI Host
Bus Adapter
312

LAN
Adapter
310

Expansion
Bus Interface
314

Graphics
Adapter
318

Audio/Video
Adapter
319

Disk
326

Tape
328

CD-
ROM
330
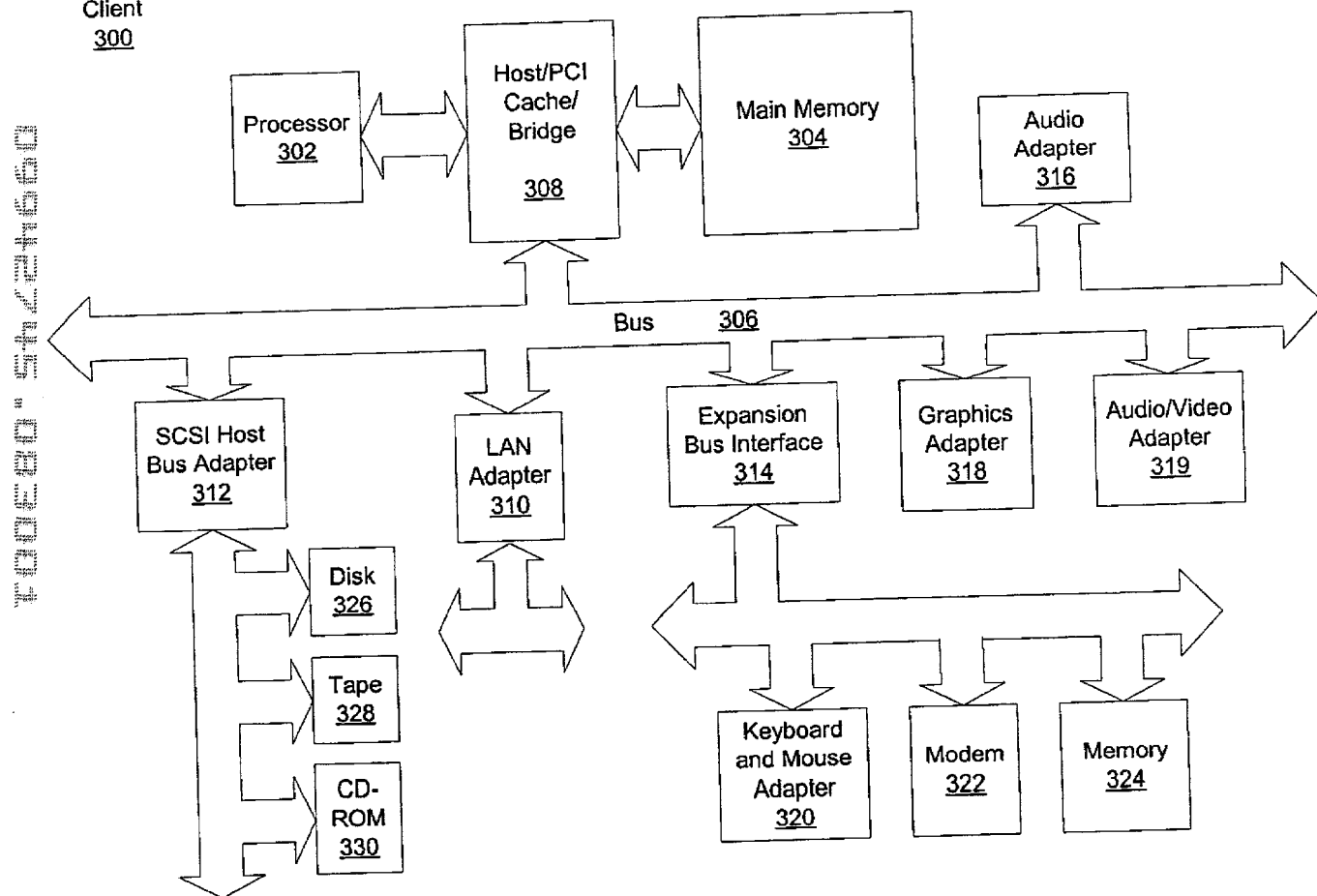
Keyboard
and Mouse
Adapter
320

Modem
322

Memory
324

# Figure 4A

Black et al.
AUS920010291US1
Method and Apparatus in a Data
Processing System for Managing
Situations from Correlated Events
Page 3 of 6

| 400 | 402 | 404 |
|-----|-----|-----|

Source → Target

# Figure 4B

408

406

Source

| Target |
| Target |
| Target |
| Target |
| Target |

410

# Figure 4C

414

412

| Source |
| Source |
| Source |

→ Target

416

# Figure 5A

Black et al.
AUS920010291US1
Method and Apparatus in a Data
Processing System for Managing
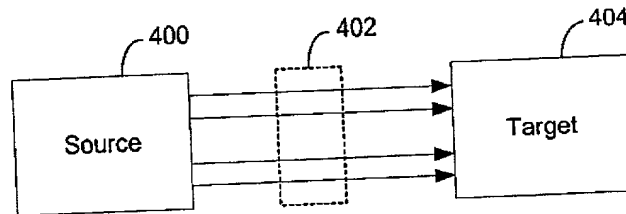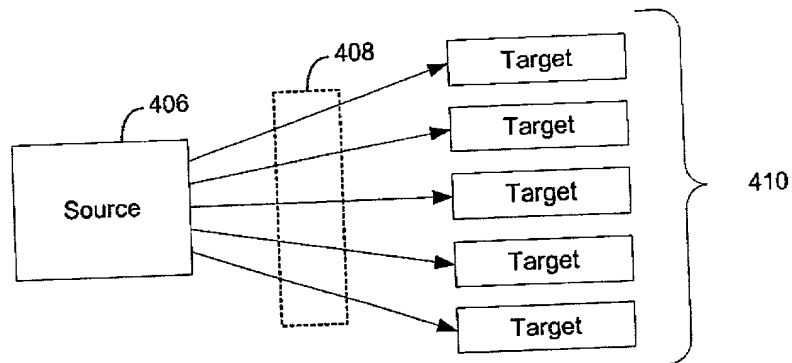Situations from Correlated Events
Page 4 of 6

500

| ALERTS | |
| --- | --- |
| ● Computer 4 has detected DoS from 66.180.200.112 ⟋502 | |
| Firewall 1 has blocked Internet access from 64.12.14.102 ⟋504 | |
| Firewall 1 has blocked Internet access from 66.12.183.200 ⟋506 | |
| Firewall 6 has blocked Internet access from 188.242.111.15 ⟋508 | |
| Firewall 2 has blocked Internet access from 214.188.144.2 ⟋510 | |

512

# Figure 5B

500

| ALERTS | |
| --- | --- |
| Firewall 6 has blocked Internet access from 208.63.252.115 (UDP Port 10,55) | |
| Firewall 6 has blocked Internet access from 208.64.203.112 ⟋516 | 514 |
| Firewall 3 has blocked Internet access from 210.15.218.102 ⟋518 | |
| ● Firewall 4 has blocked Dos from 66.180.200.112 ⟋502 | |
| Firewall 3 has blocked Internet access from 64.100.210.43 ⟋520 | |

522

# Figure 5C

500

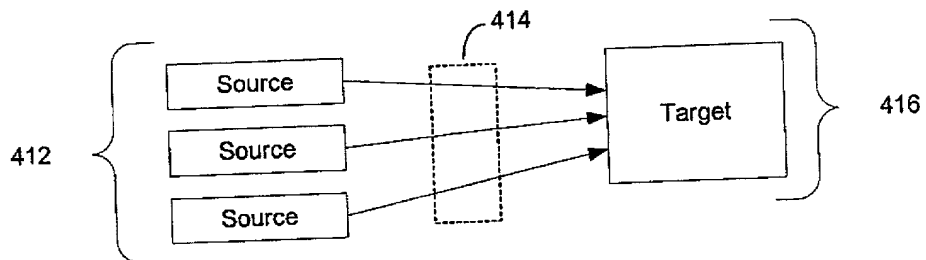| ALERTS | |
| --- | --- |
| Firewall 3 has blocked Internet access from 100.204.88.15 ⟋524 | |
| Firewall 3 has blocked Internet access from 100.204.82.106 ⟋526 | |
| Firewall 5 has blocked Internet access from 42.100.188.222 ⟋528 | |
| Firewall 6 has blocked Internet access from 66.120.222.212 ⟋530 | |
| Firewall 2 has blocked Internet access from 188.220.84.1 ⟋532 | |

# Figure 6

Black et al.
AUS920010291US1
Method and Apparatus in a Data
Processing System for Managing
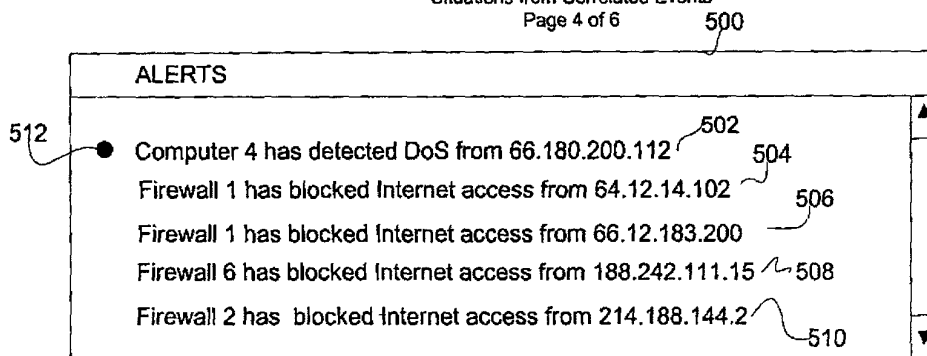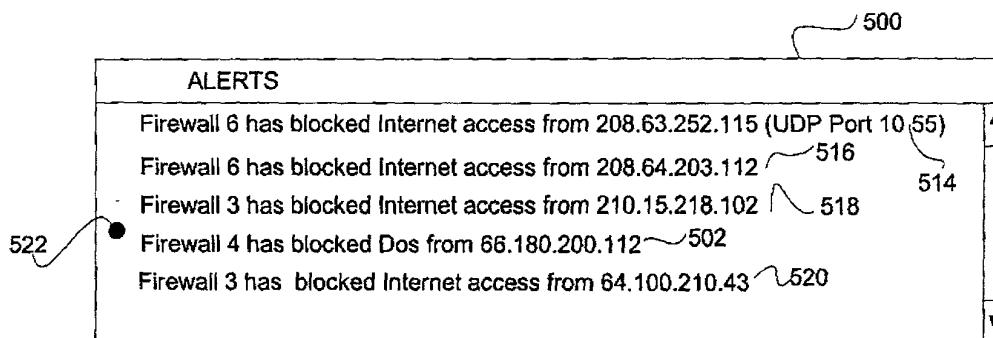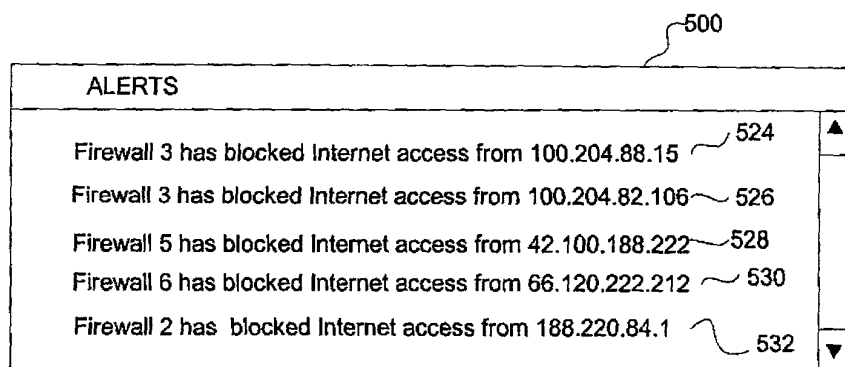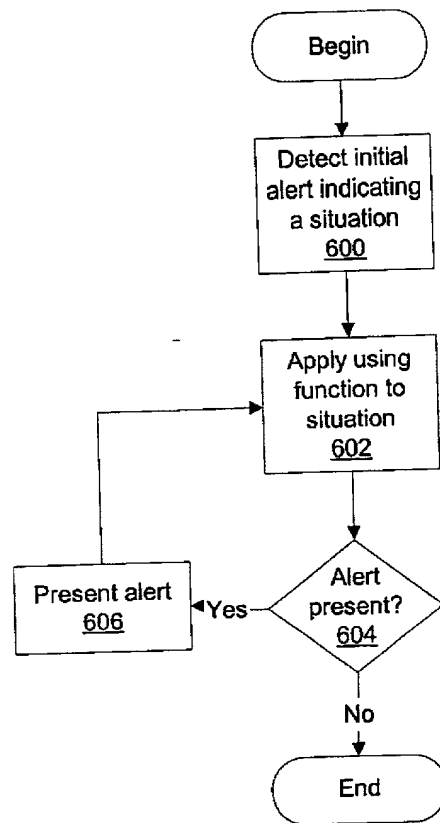Situations from Correlated Events
Page 5 of 6

```
                        ┌─────────────┐
                        │    Begin    │
                        └──────┬──────┘
                               │
                               ▼
                        ┌─────────────┐
                        │Detect initial│
                        │alert indicating│
                        │ a situation │
                        │     600     │
                        └──────┬──────┘
                               │
                               ▼
                        ┌─────────────┐
              ┌────────▶│ Apply using │
              │         │ function to │
              │         │  situation  │
              │         │     602     │
              │         └──────┬──────┘
              │                │
              │                ▼
  ┌──────────────┐         ╱───────╲
  │Present alert │◀─Yes──  ╱  Alert  ╲
  │     606      │         ╲ present? ╱
  └──────────────┘          ╲  604   ╱
                             ╲──┬──╱
                               No
                               │
                               ▼
                        ┌─────────────┐
                        │     End     │
                        └─────────────┘
```

# Figure 7

Begin

Detect event
700

First event
for situation?
702

—Yes→ Create alert
on console
706

No

Increase
severity of
situation
704

End

# Figure 8

Begin

Detect timer
expiration
800

Identify alerts for
situations
802

Select
unprocessed alert
804

Is situation
subject to
increasing time
function?
806

—No→ Adjust alert
using half-
life function
812

Yes

Yes

Adjust alert using
linear function
808

More
unprocessed
events?
810

No

End